9800513
0100513

SECRET

PART TWO

At a later date a more detailed interrogation was held with "G" and a step-by-step account of the German solution of M-209 messages containing like indicatots was studied. The following analysis should impress the seriousness of this violation.

For example: The following two messages *

Msg.#1 GGRXL JCKIY QSYLT NDOBR CTUXM KDURN NEISO LENVU etc.
Msg.#2 GGRXL JCKIY LGRBX UMDEK JYLSQ JSIRN ZEWLO BEIFJ etc.

and so on for sixty or more letters of cipher text. (This has been done with as few as forty but a considerable amount of difficulty was encountered).

Let it be assumed that ZPARENZ is contained in the top message somewhere. To locate the position of this word in the message obtain a deep sheet of data paper about thirty blocks in width and lay-out a plain alphabet across the top adding extra letters for high frequencies such as E, T, R, N, O, Z, and etc,etc. i.e.

ABCDEEEFGHIIJKLMNNOOPPQRSTTUVWXYZZZ Call this the "Table"

It will hardly be likely that this particular assumption will be found in the first few groups but for the sake of thoroughness begin at "Q" in the third group (First group of cipher text). With two strips, one a plain alphabet and one a reverse alphabet, slide one against the other until "A" is over "Q" which conversely makes "L" (First letter of cipher text of 2nd message) equal to "F". On the "Table" under

DOWNGRADE TO:
SECRET on:
CONFIDENTIAL on: 3-1-475
DECLASSIFY on:
CLASSIFIED by: DOD 5200.17 (NO)
SECRET
CA1945
APPENDED DOCUMENTS CONTAIN SPECIAL INTELLIGENCE
Authority EO
By ED NARA

the plain alphabet construct a similer continuity of letters but this time begin with "F" under "A" and repeating letters falling under repeating letters in the original plain alphabet. i.e.

ABCDEEEFGHIIJKLMNNOOPPQRSTTUVWXYZZZ
FGHIJJJKLMNNOPQRSSTTUUVWXYYZABCDEEE

Now, assuming "A" equals "S" (2nd letter of cipher text of msg. No. 1) then conversely "G" (2nd ltr. of cipher text of msg. #2.) equals "M".

Add this to the "Table" in the same maner. i.e.

ABCDEEEFGHIIJKLMNNOOPPQRSTTUVWXYZZZ
FGHIJJJKLMNNOPQRSSTTUUVWXYYZABCDEEE
MNOPQQQRSTUUVWXYZZAABBCDEFFGHIJKLLL

Continue repeating this process throughout the two messages(or at least twelve or fifteen groups) . Upon completion of the "Table" cut it into strips vertically which will provide a strip for each letter of the alphabet and extra strips for the high frequency letters.

What has been accomplished thus far is a set of strips that can be used to test any assumption throughout the message, and more than that, establish the exact location of the word assumed in the first message and the word or word-part uncovered in the second message.

To operate these strips an assumed word is spelled diagonally upward and to the right using the letters heading each strip. i.e, To try ZPARENZ take a strip headed "Z" and to the right of it and one block upwards place the

Authority E.O.
By ED NARA

strip headed with the letter "P". to the right of these two a and one more block upwards place the strip headed with the letter "A" and so on to the final "Z". Now, scrutinize horizontally down through the block of letters, that has been formed, searching for plain text. A word or word-part will appear if ZPARENZ is in the first message. (If no plain text appears try other assumptions including enciphered "Z's" at the end.) On the first strip begin with the second letter from the top and count down to the line containing what appears to be plain text. i.e. LERYZFI [illegible] count at a point twenty two lines below thw plain alphabet. The next step will be to place this assumed word and the recovered word-part in their respective positions above and below the two lines of cipher text. i.e.

ZPAR ENZ
GGRXL JCKIY QSYLT NDOBR CTUXM KDURM NEISO LENVU ETC, Msg.#1.
GGRXL JCKIY LGRBX UMDEK JYILSQ JSIRNZ[illegible]O BEIFJ ETC, Msg.#2
LERY ZFI
ZARTI L RE Z

Complete the word-part in both directions and with this added information slide the two alphabets obtaining more plain text in the first message which will be alternately used in determining more plain text in the second message. Continuing this procedure will eventually establish all the plain text of both messages. With this clear text and cipher text it is a simple matter to reconstruct the pin and lug settings. Reference was made of a group who specialized in regaining the absolute settings and who required approximately two days for this operation. There is reason to doubt this amount of time being necessary.

Authority E.O.
By ED NARA

Sofaras "G" was informed, this was the only entry to M-209 traffic; yet on the other hand the statement was made," More M-209 traffic was read than we realized." Since "like-indicators" is a more or less obscure violation it seems hardly likely that the enemy could achieve results over our estimation with this as the only entry. "G" definitely stated that no results were obtained through attacking single messages. It is difficult to believe that the enemy has not discovered, and put to use, other methodes involving only one message with violations.

Reference was made to a cryptographic section in the Foreign Office in Berlin but no information was ever obtained as to the activities of this organization. Here there is food for thought.

Daniel R. Schnabel, Jr., PFC.

Authority E.O.
By ED NARA

Authority E.O.
By ED NARA

Turning to the cryptanalytic efforts of "G" during his service in the German Army it was learned that his work, although not of the highest relative plane, was of sufficient bearing to be extremely helpful in determining the extent of enemy activity against allied communications.

Following the completion of the usual preliminary courses in cryptography and cryptanalysis (one of Fletcher Pratt's books on cryptanaysis was used as a text and possibly furnished the basis for the curriculum.) his first work was on Spanish, Portuguese, and Brazilian, presumabley, diplomatic communications. The systems used were the transposition type and the majority of Brazilian traffic was readable. Included in this training was a system indixed as EC-5 (English Code No. 5). This system was later referred to as the SLIDEX and was assumed to be a rectangle 9x12 upon which code values were written in cells located through diagraphic coordinates applied first at the top and than at the bottom. The "Slidex" was easily and regulary solved. "G" felt that this yielded a considerable amount of valuable intelligance particularly as to bombing and artillary objectives.

Some time later "G" was returned to Berlin for additional training where he studied the operation of the Hagolin Machine.

During an indefinite period "G" worked on an American strip system emanating from Iceland and the Carribbean area. Twenty fire strips, which remained the same, were used with their order changing each day. As well as could be explained a group of charts were prepared (possibly synoptic tables), lettered across the top with a plain alphabet and numbered down the side from one to twenty five. Attempts to break these messages often met with success through assuming the first word which was usually "Request" and obtaining the daily key. Later developments resulted in the use of I.B.M. cards for the purpose of eliminating

Authority E.O.
By ED NARA

impossible charts. Most of the messages proved to be practice traffic and were readable by reason of the fact that the word "practice" was usually contained therein. There was no knowledge of the strips having ever been captured, however, they were reconstructed by two other members of the staff (Stainberg and Luzius). Although cryptanalytically unimportant an occaisional literal key was recovered for amusement, one in particular was remembered as reading, "Join the Navy and See the World".

Approaching more current activities brought about the discussion of the Division Field Code where mention was made of a version ninteen or twenty one having been captured. This material in the enemy's hands was useful in solving subsequant "D.F.C's." This work covered North African traffic intercepted at Tamrmine, Sicily. The figure D.F.C. was sufficiantly secure, however the limitation of the literal version of the code enabled reading it. A particular instance of great help was a message which read, "Draw supplies at .....". And The name of the location inserted by the use of speller groups. The word length enabled the identification of the area and was a start in the reconstruction of the speller values. It was discovered that when the D.F.C. was enciphered it was done by polyalphabetic substitution using a reciprocal alphabet with a period that was always the multiple of four. It was felt by "G" and his associates that it was a grave mistake to have these period lenghts.

Other work on code traffic included the US Air Transport in Africa, which was solved. It was a two digit code not mixed with plain text. Characteristics were: the value 12 introduced figures; the value 55 introduced speller groups; the word ACCRA frequently appearred and early 1943 traffic consisted mostly of transportation of personnel. One message was recalled as having stated, "Extend all courtesy to Mrs. McArthur".

Authority E.O.
By ED NARA

The British War Office Code (W.O.C.) was reconstructed cryptanalytically and read until the code was captured in Africa. A Doctor Liedtke worked for over a year to break the superseeding system but was unsuccessful.

There was a compromised unenciphered US five-letter two part code (AC 1) still being read when "G" left Berlin.

In 1940 enciphered messages of the French Hagelin Machine (Referred to as C-36), were solved as a result of almost all messages beginning with "refer". It was concluded that this machine had fixed lugs and the kicks were always 1, 2, 4, 8, and 10. These internal settings were only changed every few months and when they were the first traffic under the new key would be sent to Berlin by curier where solution was achieved within 48 hours.

Questioning the enemy's activities on the M-209 brought the interogation up to the more recent accomplishments and developments. Insofar as "G" knew, there had been no success with this device while in Berlin and it was not until the fall of 1943 that the first break came from the result of cryptanalytic efforts. However, in June of 1943 a key list of the current month was captured in Sicily resulting in the reading of all M-209 messages in the key for that period. Apparently the loss had never been reported. One year later, 6th June 1944 (D-Day), the keys for the 6th, 7th, 8th, 9th, 10th, and 11th were captured and all pertaining traffic read.

The violation of security that finally gave the enemy their entry to our traffic cryptanalytically was messages of identical indicators. Although having been done with less, messages of 60 or more letters of cipher text and like indicators could be solved by two men in a couple of hours. Strips were prepared by working one message against the other while pushing through an assumed word. "ZPARENZ" was used to a great extent and almost always was the opening wedge. As

Authority E.O. By ED NARA

soon as the position of this stereotype was located the rest of the two messages fell apart quite readily. The pin and lug set-up was then sent to another group who established the absolute setings. This final operation was reported to require on the average, two days. There was another method of reconstructing the absolute setting in a few hours, through the use of an indicator from the third message under certain conditions which "G" was unable to make clear. There was recalled a period in May 1944 when the indicators were found on nine consecutive days and all traffic was read for eight of those days.

It was "G's" impression that more M-209 traffic was being read than was imagined; this was due to breaches of security and not the system. He felt, however, considering American traffic as a whole, that their success was not what we probably anticipated.

Complete failure was encountered in attempts on the US "Big Machine" and American transposition traffic. In regard to the latter, three messages of identical length in the same key were unsuccessfully looked for as this was the break in the Brazilian traffic.

"G" knew of another cryptographic section in the Foreign Offices but was unaware of the nature of the work perfomed by this organization.

This prisoner spoke excellant English and most of his information was precise and clear; however, he did have some difficulty with technical German cryptographic terms. He was fully cooperative and aswered all questions freely and with apparent honesty. This cooperation was motivated by the belief that Germany had no chance of winning the war and that the sooner it was over the better.

Daniel Schnable, Jr. P.F.C.

Authority E.O.
By ED NARA

SECRET

PROPROSED APPENDAGE TO FAAA SOP

RESULTS DESIRED: TO EMPLOY THE M-209 WITH SIMILER SECURITY OF THE ONE-TIME-PAD

PROCEDURE;

A. PIN SETTINGS SHOULD BE CONSTRUCTED IN THE USUAL MANER, I.E. THE NUMBER OF ACTIVE AND/OR INACTIVE PINS SHOULD NOT EXCEED 60% OR FALL BELOW 40% OF THE NUMBER OF PINS ON THE RESPECTIVE WHEELS.

B. LUG SETTINGS SHOULD ALSO FALL WITHIN THE PRESCRIBED LIMITATIONS WITH THE EXCEPTION OF THE PROPROSAL TO ESTABLISH TWO HIGH KICK WHEELS RATHER THAN THE CONVENTIONAL ONE. I.E. CONTINUE UNDER THE REQUIREMENTS OF OBTAINING ANY TOTAL FROM ONE TO TWENTY SEVEN THROUGH THE VARIOUS COMBINATIONS OF LUG SETTINGS. THIS OF COURSE WILL REDUCE THE NUMBER OF POSSIBILITIES FOR VARIED SET-UPS BUT SHOULD BE OF LITTLE CONSEQUENCE IN THE FACE OF THE ADDED SECURITY. (SEE PLATE ONE)

C. ASSUMING X, Y, AND Z WANTS INDIVIDUAL SECURITY WHEN COMMUNICATING WITH A, B, C, D, E, AND F WITHOUT THE NECESSITY OF CARRYING INSTRUCTIONS ON FURTHER CHANGES OF PIN AND LUG SET-UPS OR TIME CONSUMING ALTERATIONS THE FOLLOWING IS PROPOSED. (SEE PLATE TWO)

D. THE FIRST OPERATION, IN ANY EVENT, WILL BE TO OBTAIN AN INTERNAL INDICATOR IN THE CUSTOMARY MANER AND INSERT IT IN THE MACHINE WITH THE COUNTER AT ZERO. FOR ALL MESSAGES EMNATING FROM "X" THE WHEELS WILL BE ADVANCED AS A GROUP TO A POINT WHERE THE COUNTER REALS 110; FROM "Y" THE WHEELS WILL BE ADVANCED UNTIL THE COUNTER READS 220; AND FROM "Z" THE WHEELS WILL BE ADVANCED UNTIL THE COUNTER READS 330.

E. AS X,Y, AND Z WAS NUMBERED 1, 2, AND 3,LIKEWISE CONSIDER A TO F AS BEING NUMBERED FROM 1 TO 6 RESPECTIVILY. IF X IS TO COMMUNICATE WITH C (NUMBER 3) HE WILL FIRST ROTATE THE WHEELS, AS A GROUP, UNTIL THE INDICATOR REALS 110; THEN ADVANCE THE FIRST WHEEL (26 WHEEL) SINGLY THREE POSITIONS;ADVANCE THE NEXT WHEEL (25 WHEEL) SINGLY FOUR POSITIONS; ADVANCE THE NEXT WHEEL (23 WHEEL) SINGLY FIVE POSITIONS; ADVANCE THE NEXT WHEEL (21 WHEEL) SINGLY SIX POSITIONS; ADVANCE THE NEXT WHEEL (19 WHEEL) SINGLY ONE POSITION; AND FINALLY THE SIXTH OR LAST WHEEL (17 WHEEL) TWO POSITIONS. THE MACHINE IS NOW READY FOR ENCIPHERING. IN EACH INSTANCE, AFTER THE WHEELS AS A GROUP HAVE BEEN SET AT 110, 220, OR 330, DEPENDING UPON WHOM IS SENDING, THE WHEELS WILL BE INDIVIDUALLY ADVANCED IN A MANER DETERMINED BY THE NUMBER OF THE RECIPIENT. E.G.

SECRET

Authority E.O.
By ED NARA

THE FOLLOWING TABLE WILL CLARIFY THE INDIVIDUAL WHEEL RESET;

ADJUST AS FOLLOWS	26	25	23	21	19	17
WHEN SENDING TO A (1)	1	2	3	4	5	6
" " " B (2)	2	3	4	5	6	1
" " " C (3)	3	4	5	6	1	2
" " " D (4)	4	5	6	1	2	3
" " " E (5)	5	6	1	2	3	4
" " " F (6)	6	1	2	3	4	5

E. THIS ARRANGEMENT OF ALTERING THE SET-UP REQUIRES NO WRITTEN INSTRUCTIONS. EACH ADJUSTMENT IS MADE ACCORDING TO THE NUMBER EACH INDIVIDUAL GROUP REPRESENTS AND CAN BE EASI;Y RETAINED MENTALLY.

G. AT ANY TIME THAT A PIN AND LUG SET UP MIGHT BE CAPTURED CURRENT MESSAGES COULD NOT BE DECIPHERED WITH OUT KNOWLEDGE OF THE RESETS. EVEN IN THE EVENT OF THE MANY VIOLATIONS OF SECURITY, WHICH GIVE THE ENEMY WEDGES INTO OUR TRAFFIC, COULD CRYPTANALYTIC ACTIVITY BE OF ANY PRACTICAL VALUE SINCE THE RESETS PREVENT RECONSTRUCTION OF ANY ABSOLUTE SETTINGS THAT WOULD EFFECTIVE AGAINST READING MESSAGES TO OTHER GROUPS. NEITHER WOULD LIKE INDICATORS BE OF ANY VALUE, UNLESS VIOLATION OCCURED WITHIN MESSAGES TO ONE SPECIFIC GROUP, SINCE THE RESET OPERATION WOULD DESTRY ANY RELATIVITY BETWEEN THE TWO. (SEE PLATE 3)

IN CONCLUSION: THE TIME ELEMENT, IF CONSIDERED, IN THIS ADDITIONAL ADJUSTMENT WILL REQUIRE APPROXIMATELY TWENTY FIVE SECONDS. NO MORE ACCURACY WILL BE REQUIRED IN THE ORIGINAL SET-UP THAN IN THE CONVENTIONAL SYSTEM AS THE RESETS DO NOT AMPLIFY ERRORS. MINUTE ERRORS IN THE PREPARATION OF THE MACHINE FOR ENCODERING DO NOT ALWAYS RENDER A MESSAGE UNDECIPHERABLE; NOR TO ANY LESSER DEGREE WILL THIS BE TRUE AS A RESULT OF THE RESETS.

PFC DANIEL R SCHNABEL
13154897

Authority E.O.
By ED NARA